AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1 CONTRACT ID CODE	PAGE OF PAGES
J	1 | 12

2 AMENDMENT/MODIFICATION NO	3 EFFECTIVE DATE	4 REQUISITION/PURCHASE REQ NO	5 PROJECT NO (If applicable)
P00003	02-Apr-2019	SEE SCHEDULE	

6 ISSUED BY	CODE	7 ADMINISTERED BY (If other than item 6)	CODE
NAVAL INFORMATION WARFARE CENTER PAC FIC (b)(6) CODE 22530 (b)(6) @NAVY MIL 53560 HULL ST SAN DIEGO CA 92152-5001	N66001	See Item 6	

8. NAME AND ADDRESS OF CONTRACTOR (No., Street, County, State and Zip Code)		
FORCEPO NT FEDERAL LLC 12950 WORLDGATE DR STE 600 HERNDON VA 20170-6024		9A. AMENDMENT OF SOLICITATION NO.
		9B. DATED (SEE ITEM 11)
	X	10A. MOD. OF CONTRACT/ORDER NO. N6600117C0031
	X	10B. DATED (SEE ITEM 13) 22-Aug-2017
CODE 029J2	FACILITY CODE	

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offer ☐ is extended, ☐ is not extended.

Offer must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended by one of the following methods: (a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

☐ A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.

☐ B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(B).

X C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
Mutual Agreement of the Parties.

☐ D. OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor ☐ is not, ☒ is required to sign this document and return 1 copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)
Modification Control Number: (b)(6)
This modification revises the Performance Work Statement and the DD254. All other terms and conditions remain unchanged. Please see the following page(s).

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print)	16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)
	JENN FER J. ROESNER / CONTRACT SPECIALIST TEL: 619-553-5283 EMA L: jennifer roesner@navy.mil

15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA	16C. DATE SIGNED
(Signature of person authorized to sign)		BY Jennifer Roesner (Signature of Contracting Officer)	04-Apr-2019

SECTION SF 30 BLOCK 14 CONTINUATION PAGE

SUMMARY OF CHANGES

SECTION SF 1449 - CONTINUATION SHEET

TABLE OF CONTENTS

The Table of Contents has changed from:

Exhibit/Attachment Table of Contents

DOCUMENT TYPE	DESCRIPTION	PAGES	DATE
Exhibit A	Contract Data Requirements List (CDRL)	13	05-MAY-2017
Attachment 1	Performance Requirements Summary (PRS)	7	09-JAN-2017
Attachment 2	DD-254 REV 1	4	26-JUL-2018

to:

Exhibit/Attachment Table of Contents

DOCUMENT TYPE	DESCRIPTION	PAGES	DATE
Exhibit A	Contract Data Requirements List (CDRL)	13	05-MAY-2017
Attachment 1	Performance Requirements Summary (PRS)	7	09-JAN-2017
Attachment 2	DD-254 Rev 2	5	31-JAN-2019

The following have been modified:

PERFORMANCE WORK STATEMENT

TITLE: United States Air Force (USAF) New Command and Control (C2) Facility Installation, Integration, and Operations

1.1 SCOPE

The purpose of this task is to provide systems engineering and integration support to facilitate the SPAWAR Systems Center, Pacific (SSC Pacific) Government team in the design and installation of the IT infrastructure for a new C2 facility throughout the period of performance. Services required include site survey, systems architecture design, deployment, installation guidance, training, testing and engineering expertise in the operation and maintenance of the multi-level security system, Trusted Thin Client.

1.2 BACKGROUND

The USAF is building a new Command and Control Facility at Offutt Air Force Base, Nebraska. The U.S. Army Corp of Engineers is executing the military construction on behalf of the USAF. Space and Naval Warfare Systems Center, Pacific (SSC Pacific) has accepted tasking to design, procure, integrate, and install a C4I/IT infrastructure and transition C4I/IT systems into the new Facility. The design vision is to build a state of the art facility with the flexibility to support operations for the next 50 years. SSC Pacific is following its shore installation process which defines engineering phases and distinct deliverables during each phase leading to a Sponsor review and acceptance before proceeding to the next phase.

2.0 APPLICABLE DOCUMENTS

2.1 Department of Defense (DoD)/Intelligence Community (IC) Documents:

- 2.1.1 SPAWAR M-4720.1, Shore Installation Process Handbook v4.0, 12 Nov 14
- 2.1.2 DoD 8570.01-M, Information Assurance Workforce Improvement Program
- 2.1.3 DISA Security Technical Implementation Guides (STIGs)
- 2.1.4 SECNAVINST 5510.30 (Series), Department of Navy Personnel Security Program
- 2.1.5 SECNAVINST 5510.36 (Series), Department of Navy Information Security Program
- 2.1.6 OPNAVINST F3300.53C (Series), Navy Antiterrorism Program
- 2.1.7 DOD 5200.01 Volumes 1 through 4 (Series), DOD Security Program
- 2.1.8 DOD 5220.22-M (Series), National Industrial Security Program Operating Manual (NISPOM)
- 2.1.9 National Security Decision Directive 298 (Series), National Operations Security Program (NSDD) 298
- 2.1.10 DOD 5205.02 (Series), DOD Operations Security (OPSEC) Program
- 2.1.11 OPNAVINST 3432.1 (Series), DON Operations Security
- 2.1.12 SPAWARINST 3432.1 (Series), Operations Security Policy

2.2 Availability of DoD/IC Documents.

Documents listed above are available from the Contracting Officer's Representative.

3.0 TECHNICAL REQUIREMENTS

The contractor shall provide on-site engineering expertise, guidance and recommendations in the installation, accreditation, training, operation and maintenance of the new C2 Facility installation as well as the current prototype Trusted Thin Client (TTC) solution.

3.1 Base Period

Base Period overview/summary: The base period will provide design finalization with low level documentation and POA&M. It will include development of Accreditation Package Plan and initiate installation (data center install and configuration). The contractor tasking details are addressed below.

Duties performed and work products are all at the SECRET level and below. All individuals supporting this task should be cleared to the TOP SECRET/SCI level because this on-site work is performed in an active SCIF area.

3.1.1 Trusted Thin Client Prototype. The contractor shall initially operate and maintain the current prototype environment of Trusted Thin Client consisting of two distribution consoles, approximately thirty clients, two gray network Active Directory (AD)/Domain Name System (DNS)/Dynamic Host Configuration Protocol

(DHCP) servers, a log server and others as necessary. As the new system is installed the contractor shall perform the same duties on the production installation in the new facility. This shall be accomplished in accordance with project requirements, TTC manufacturer best practices, and US Government Information Assurance requirements.

While augmenting existing TTC Administrator and User Guides, the on-site engineering expert(s) shall be responsible for producing 'as-built' documentation for the TTC prototype and pre-implementation for the production environment. The contractor shall be responsible for reviewing all documentation produced for the new installation to provide inputs to cover all facets of the installations. The Government will review and approve documentation prior to release to the customer. The documentation shall include, but is not limited to applicable drawings, installation and operation and maintenance documentation for the contractor tasking listed below:

- Technical Project Management (Oversight, Resourcing, Budgeting, Scheduling, Risk Mitigation)

- Pre-Onsite support
  - Kickoff and coordination

- Systems Architecture
  - Architect, Design, Build and provide implementation and operational guidance for use case and outcome based TTC solutions that incorporate Forcepoint and 3rd party products.
  - Present strategy and integrated vision aligned to business case scenarios.
  - Develop Strategy and Roadmap deliverables to meet technical solutions.
  - Work with Engineering to stand-up defined architectures and feedback on "Lessons learned" and "Best Practices."
  - Effectively communicate solutions architecture to the entire team.
  - Monitor build process and provide version guidance throughout the program. lifecycle to ensure seamless integration across the platforms.
  - Monitor and provide guidance for proper validation testing.

- Onsite Subject Matter Expert(s) (SMEs) Omaha NE. The onsite engineering expert(s) shall:
  - Assist the System Architect in design, analysis, engineering, integration, and operational activities during all phases of the project lifecycle.
  - Provide on-site vendor liason representative to SPAWAR System Center Pacific, USSTRATCOM, DIA and DISA.
  - Provide consultation services and reach back capability to leverage development and engineering services from the TTC Manufacturer
  - Provide Requirement Analysis and Design Review
  - Provide Review Low Level Design Document
  - Maintain and Operate SPAWAR lab system that will be used to test and prototype designs for the new C2 Facility.

- Pre-Deployment
  - Provide on-site survey in preparation for initial system installation
  - Develop installation plan
  - Develop Authorization and Accreditation (A&A) plan

- A&A Support
  - Assist with the Body of Evidence documentation for system accreditation.
  - Gather information for the creation of System Security Plan (SSP) and System Controls Traceability Matrix (SCTM)
  - Gather information for the creation of the Security Test and Evaluation (ST&E)

Procedures
- Create initial draft of SSP, SCTM and ST&E Plan
- Assist site in conducting on site ST&E event
- Assist in creating ST&E test report and Plan of Action and Milestones (POA&M) if necessary

Duties performed and work products are all at the SECRET level and below. All individuals supporting this task should be cleared to the TOP SECRET/SCI level because this on-site work is performed in an active SCIF area.

3.1.2 TTC Software Installation

The contractor shall provide initial settings for proper / optimal system operations:

- System Firmware / Bios settings, versions compatibility with TTC product to maintain current and future security guidelines
- Hard drive Redundant Array of Inexpensive Disks (RAID settings (software install, log partitions, etc.)
- Settings for system interaction with other systems (e.g. Java web console mouse pointer issues, external monitoring)

The contractor shall provide installation guidance:

- Best practices (ideal vs real world, mitigations for conflicts in security postures/ requirements)
- Tradeoffs (memory, CPU cores, disk space such as solid-state drive (SSD) vs. traditional)
- Clients

The contractor shall provide configuration:

- Prototype installation vs Production deployment
- Conform (as much as possible) to network security guidelines for networks the system might not normally be deployed on. (Unclassified – prototype with needs for ACAS scanning, AV, HIPS, HBSS, DLP). This also applies to the gray network servers (AD, DNS, DHCP and Log/Monitoring servers)
- Apply Security Technical Implementation Guides (STIGs) and applying patches and mitigating vulnerabilities to machines and SSC Pacific lab spaces
- Provide guidance and support for how the system would differ when transitioned to a production environment
- Corporate Branding (Backgrounds, Icons etc.)
- Thin Client specific installations and configurations (Jabber, Streaming media etc.)
- Multiple monitor configurations (1-4).
- Webcams, CAC readers, Headsets
- Support the use of multiple smartcard/token readers for different enclaves simultaneously
- Support centralized administration of all system components
- Support automatic updates for system components with no need for desk side support
- Support single wire to client for all enclave access
- Support automatic failover of clients between datacenters in the event of datacenter failure
- Support Add, Change, or Remove enclave connections to the Multiple Levels of Security (MLS) without desk side support
- Support access to remote Windows virtual machines hosted within a Virtual Desktop Infrastructure (VDI).
- Support Windows 10 VDI infrastructure through FIPS compliant connection brokers.

- Support low power clients (total end user position power budget is 300 watts, two monitors, Keyboard, Video and Mouse (KVM) switch, one MLS client, one zero client, speakers, phones, etc.)

The contractor shall provide installation:

- Validate network and backend infrastructure technical information
- Validate final integration plans
- Verify system installation
- Integrate with network and backend infrastructure for each enclave
- Perform end-to-end functional testing including service integration testing for Active Directory, SMTP, DNS, DHCP and backend infrastructure.

Duties performed and work products are all at the SECRET level and below. All individuals supporting this task should be cleared to the TOP SECRET/SCI level because this on-site work is performed in an active SCIF area.

3.2 Option Period 1

Option 1 Period overview/summary: The option 1 period will continue and complete the installation (finalized data center configurations and install of end user client devices), provide System Operations Verification Test (SOVT) documentation for overall system install and configuration, and final accreditation package. The contractor tasking details are addressed below.

3.2.1 Trusted Thin Client Prototype. The contractor shall initially operate and maintain the current prototype environment of Trusted Thin Client consisting of two distribution consoles, approximately thirty clients, two gray network Active Directory (AD)/Domain Name System (DNS)/Dynamic Host Configuration Protocol (DHCP) servers, a log server and others as necessary. As the new system is installed the contractor shall perform the same duties on the production installation in the new facility. This shall be accomplished in accordance with project requirements, TTC manufacturer best practices, and US Government Information Assurance requirements.

While augmenting existing TTC Administrator and User Guides, the on-site engineering expert(s) shall be responsible for producing 'as-built' documentation for the TTC prototype and pre-implementation for the production environment. The contractor shall be responsible for reviewing all documentation produced for the new installation to provide inputs to cover all facets of the installations. The Government will review and approve documentation prior to release to the customer. The documentation shall include, but is not limited to applicable drawings, installation and operation and maintenance documentation for the contractor tasking listed below:

- Technical Project Management (Oversight, Resourcing, Budgeting, Scheduling, Risk Mitigation)

- Systems Architecture.
  - Architect, Design, Build and provide implementation and operational guidance for use case and outcome based TTC solutions that incorporate Forcepoint and 3rd party products.
  - Present strategy and integrated vision aligned to business case scenarios
  - Develop Strategy and Roadmap deliverables to meet technical solutions
  - Work with Engineering to stand-up defined architectures and feedback on "Lessons learned" and "Best Practices."
  - Effectively communicate solutions architecture to the entire team
  - Monitor build process and provide version guidance throughout the program lifecycle to ensure seamless integration across the platforms
  - Monitor and provide guidance for proper validation testing

- Onsite Subject Matter Expert(s) (SMEs) Omaha NE. The onsite engineering experts shall:

- Provide design, analysis, engineering, integration, and operational activities during all phases of the project lifecycle.
- Provide consultation services and reach back capability to leverage development and engineering services from the TTC Manufacturer.
- Maintain and Operate SPAWAR lab system that will be used to test and prototype designs for the new C2 Facility.

- A&A Support
  - Assist with the Body of Evidence documentation for system accreditation.
  - Gather information for the creation of SSP and SCTM
  - Gather information for the creation of the ST&E Procedures
  - Finalize drafts of SSP, SCTM and ST&E Plan

Duties performed and work products are all at the SECRET level and below. All individuals supporting this task should be cleared to the TOP SECRET/SCI level because this on-site work is performed in an active SCIF area.

3.2.2 TTC Software Installation

The contractor shall provide initial settings for proper / optimal system operations:

- System Firmware / Bios settings, versions compatibility with TTC product to maintain current and future security guidelines
- Hard drive Redundant Array of Inexpensive Disks (RAID settings (software install, log partitions, etc.)
- Settings for system interaction with other systems (e.g. Java web console mouse pointer issues, external monitoring)

The contractor shall provide installation guidance:

- Best practices (ideal vs real world, mitigations for conflicts in security postures/ requirements)
- Tradeoffs (memory, CPU cores, disk space such as solid-state drive (SSD) vs. traditional)
- Clients

The contractor shall provide configuration:

- Prototype installation vs Production deployment
- Conform (as much as possible) to network security guidelines for networks the system might not normally be deployed on. (Unclassified – prototype with needs for ACAS scanning, AV, HIPS, HBSS, DLP). This also applies to the gray network servers (AD, DNS, DHCP and Log/Monitoring servers)
- Apply Security Technical Implementation Guides (STIGs) and applying patches and mitigating vulnerabilities to machines and SSC Pacific lab spaces
- Provide guidance and support for how the system would differ when transitioned to a production environment
- Corporate Branding (Backgrounds, Icons etc.)
- Thin Client specific installations and configurations (Jabber, Streaming media etc.)
- Multiple monitor configurations (1-4).
- Webcams, CAC readers, Headsets
- Support the use of multiple smartcard/token readers for different enclaves simultaneously
- Support centralized administration of all system components
- Support automatic updates for system components with no need for desk side support

- Support single wire to client for all enclave access
- Support automatic failover of clients between datacenters in the event of datacenter failure
- Support Add, Change, or Remove enclave connections to the Multiple Levels of Security (MLS) without desk side support
- Support access to remote Windows virtual machines hosted within a Virtual Desktop Infrastructure (VDI).
- Support Windows 10 VDI infrastructure through FIPS compliant connection brokers.
- Support low power clients (total end user position power budget is 300 watts, two monitors, Keyboard, Video and Mouse (KVM) switch, one MLS client, one zero client, speakers, phones, etc.)

The contractor shall provide installation:

- Validate network and backend infrastructure technical information
- Validate final integration plans
- Verify system installation
- Integrate with network and backend infrastructure for each enclave
- Perform end-to-end functional testing including service integration testing for Active Directory, SMTP, DNS, DHCP and backend infrastructure.
- Provide system training and familiarization for site specific implementation.

Duties performed and work products are all at the SECRET level and below. All individuals supporting this task should be cleared to the TOP SECRET/SCI level because this on-site work is performed in an active SCIF area.

3.2.3 Operational Testing.

The contractor shall ensure operational verification to installed network configurations and installation to include:

- Development of training plans
- Development of System Operational Verification Tests (SOVTs)

Duties performed and work products are all at the SECRET level and below. All individuals supporting this task should be cleared to the TOP SECRET/SCI level because this on-site work is performed in an active SCIF area.

3.2.4 TTC Software Operation and Maintenance

The contractor shall provide operations and maintenance of TTC Software until transition to customer for operations:

- Operate and maintain on a daily basis the Prototype test bed system, Pre- installation and check out system and production systems prior to customer turnover
- Create and maintain gray network AD Server integration with TTC, maintain synchronization with Prototype VDI AD for users accounts, group policies to maximum extent
- Provide guidance on establishment and maintenance of a gray network AD integration with TTC to support multiple enclaves on the gray network AD
- Provide security interaction between TTC and gray network, separation of admin duties amongst different enclaves
- Provide guidance on monitoring and management of Distribution Consoles from within and without customer's site (Co-Management strategy requirement)
- Maintain environment and software with latest patches, firmware, security updates
- Maintain hardware (servers and clients)

Duties performed and work products are all at the SECRET level and below. All individuals supporting this task should be cleared to the TOP SECRET/SCI level because this on-site work is performed in an active SCIF area.

3.2.5 TTC Software Integration Testing

The contractor shall provide software integration testing:

- Coordinate with VDI testing to identify common criteria, scenarios
- Provide recommendations, if any, to optimize VDI environment for TTC where practical, while meeting security and customer specific requirements.
- Provide tailored testing (prototype vs production) with supporting documentation.
- Integrate TTC with Enterprise Monitoring software such as Solarwinds, McAfee, and Security Information and Event Management (SIEM).

Duties performed and work products are all at the SECRET level and below. All individuals supporting this task should be cleared to the TOP SECRET/SCI level because this on-site work is performed in an active SCIF area.

3.3 Option Periods 2-3

Option 2-3 Periods overview/summary: The option 2-3 periods will result in final as-built drawings, configuration and other documentation. The tech refresh plan/software upgrades recommendations will be initiated and completed. The training and transition to operations will be initiated and completed. The contractor tasking details are addressed below.

Duties performed and work products are all at the SECRET level and below. All individuals supporting this task should be cleared to the TOP SECRET/SCI level because this on-site work is performed in an active SCIF area.

3.3.1 Trusted Thin Client Prototype. The contractor shall initially operate and maintain the current prototype environment of Trusted Thin Client consisting of two distribution consoles, approximately thirty clients, two gray network Active Directory (AD)/Domain Name System (DNS)/Dynamic Host Configuration Protocol (DHCP) servers, a log server and others as necessary. As the new system is installed the contractor shall perform the same duties on the production installation in the new facility. This shall be accomplished in accordance with project requirements, TTC manufacturer best practices, and US Government Information Assurance requirements.

While augmenting existing TTC Administrator and User Guides, the on-site engineering expert(s) shall be responsible for producing 'as-built' documentation for the TTC prototype and pre-implementation for the production environment. The contractor shall be responsible for reviewing all documentation produced for the new installation to provide inputs to cover all facets of the installations. The Government will review and approve documentation prior to release to the customer. The documentation shall include, but is not limited to applicable drawings, installation and operation and maintenance documentation for the contractor tasking listed below:

- Technical Project Management (Oversight, Resourcing, Budgeting, Scheduling, Risk Mitigation)
- Onsite Subject Matter Expert(s) (SMEs) Omaha NE. The onsite engineering expert(s) shall:
  - Provide design, analysis, engineering, integration, and operational activities during all phases of the project lifecycle.
  - Provide consultation services and reach back capability to leverage development and engineering services from the TTC Manufacturer
  - Maintain and Operate SPAWAR lab system that will be used to test and prototype designs for the new C2 Facility.
- A&A Support

- Assist with the Body of Evidence documentation for system accreditation.
- Gather and document information to maintain accuracy of SSP and SCTM
- Gather and document information to maintain accuracy of the ST&E Procedures
- Assist in creating ST&E test report and Plan of Action and Milestones (POA&M) if necessary

Duties performed and work products are all at the SECRET level and below. All individuals supporting this task should be cleared to the TOP SECRET/SCI level because this on-site work is performed in an active SCIF area.

3.3.2 TTC Software Operation and Maintenance

The contractor shall provide operations and maintenance of TTC Software until transition to customer for operations:

- Operate and maintain on a daily basis the Prototype test bed system, Pre- installation and check out system and production systems prior to customer turnover
- Create and maintain gray network AD Server integration with TTC, maintain synchronization with Prototype VDI AD for users accounts, group policies to maximum extent
- Provide guidance on establishment and maintenance of a gray network AD integration with TTC to support multiple enclaves on the gray network AD
- Provide security interaction between TTC and gray network, separation of admin duties amongst different enclaves
- Provide guidance on monitoring and management of Distribution Consoles from within and without customer's site (Co-Management strategy requirement)
- Maintain environment and software with latest patches, firmware, security updates
- Maintain hardware (servers and clients)

Duties performed and work products are all at the SECRET level and below. All individuals supporting this task should be cleared to the TOP SECRET/SCI level because this on-site work is performed in an active SCIF area.

3.3.3 Transition to Operations. The contractor shall orient system operators to installed network configurations and installation to include:

- Execution of training plans
- Execution of System Operational Verification Tests (SOVTs)
- Documentation of Technical Refresh Plans and final software upgrade recommendations

Duties performed and work products are all at the SECRET level and below. All individuals supporting this task should be cleared to the TOP SECRET/SCI level because this on-site work is performed in an active SCIF area.

4.0 CYBER SECURITY WORKFORCE

All task personnel operating SSC Pacific lab equipment shall be certified at information assurance technical level II (IAT II) for their respective network and computing environments. CSWF training and certification requirements are prescribed in DoD 8570.01-M, Information Assurance Workforce Improvement Program. The contractor shall report CSWF training and certification status and compliance as part of Contractor/Personnel Roster.

The contractor shall ensure that personnel accessing information systems have the proper and current IA certification to perform IA functions identified in the technical requirements section of this PWS in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program. The Contractor shall meet applicable information assurance certification requirements, including (a) DoD-approved IA workforce certifications appropriate for each specified category and level and (b) appropriate operating system

certification for information assurance technical positions as required by DoD 8570.01-M. Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions.

The contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions, reporting current IA certification status and compliance using CDRL Contractor Roster, DI-MGMT-81596 in the format prescribed by the Technical Point of Contact.

5.0 DATA DELIVERABLES

Data deliverables shall be as specified in the attached CDRL, DD1423.

6.0 TRAVEL

Performer(s) are authorized travel costs to the performance site at Offutt Air Force Base, NE. Travel is anticipated for meetings, documentation, testing, configuration, and installation tasks in accordance with paragraph 3.0 during the base and option periods.

7.0 GOVERNMENT FURNISHED PROPERTY (GFP) AND ACCESS:

GFP is not anticipated. The Government will provide access to facilities, equipment, and technical information for the performance of this task, to include full time access to administrative seats with computers and internet connectivity in the SSC Pacific lab spaces at OFFUTT AFB, NE.

8.0 OTHER

8.1 Security. ***Work performed and work products are all at the SECRET level and below. All individuals supporting this task should be cleared to the TOP SECRET/SCI level because on-site work performed in the new C2F will be predominately in active SCIF areas. The contractor shall provide a Top Secret/SCI- cleared escort for any individual not cleared TS/SCI. All individuals supporting this task must be cleared to the SECRET level because on-site work will require access to secret information. The contractor will not be producing any TOP SECRET/SCI level deliverables. Contractor personnel assigned to this effort who require access to SCI data and spaces must possess a current Single Scope Background Investigation (SSBI) with Intelligence Community (IC) Directive 704 (ICD 704) eligibility (which replaced Director of Central Intelligence Directive (DCID) 6/4 eligibility).***

Although there is no requirement for the contractor to access NATO on this contract per Naval Intelligence Security Policy Directive 17-008 those contractors that have SCI access and those cleared SCI with JWICS or SIPRnet accounts shall be North Atlantic Treaty Organization (NATO) read-on and complete the derivative classification training prior to being granted access to JWICS/SIPRnet; training is provided by the facility security officer. Specific requirements provided in the Department of Defense Contract Security Classification Specification, DD Form 254.

Contractors performing tasks at the TS or below level without SCI access also need to be NATO read-on because of requirements imposed by USSTRATCOM for personnel requiring access to SIPRnet. Specific requirements provided in the Department of Contract Security Classification Specification, DD Form 254.

Anti-Terrorism/force Protection **(AT/FP)** briefings are required for all personnel (military, DOD civilian, and contractor) prior to commencement of foreign travel. Contractor employees must receive the AT/FP briefing annually. The briefing is available at Joint Knowledge Online (JKO): https://jkodirect.jten mil (prefix): JS; course number: US007; title: Level 1 Anti-terrorism awareness training, if experiencing problems accessing this website contact ssc_fortrav@navy.mil. note: per OPNAVINST F3300.53C contractor employees must receive the AT/FP briefing annually.

As required by National Industrial Security Program Operating Manual (NISPOM) Chapter 1, Section 3, contractors are required to report certain events that have an impact on: 1) the status of the facility clearance (FCL); 2) the status of an employee's personnel clearance (PCL); 3) the proper safeguarding of classified information; 4) or an indication that classified information has been lost or compromised. Contractors working under SSC Pacific contracts will ensure information pertaining to assigned contractor personnel are reported to the Contracting Officer Representative (COR)/Technical Point of Contact (TPOC), the Contracting Specialist, and the Security's COR in addition to notifying appropriate agencies such as Cognizant Security Agency (CSA), Cognizant Security Office (CSO), or Department Of Defense Central Adjudication Facility (DODCAF) when that information relates to the denial, suspension, or revocation of a security clearance of any assigned personnel; any adverse information on an assigned employee's continued suitability for continued access to classified access; any instance of loss or compromise, or suspected loss or compromise, of classified information; actual, probable or possible espionage, sabotage, or subversive information; or any other circumstances of a security nature that would affect the contractor's operation while working under SSC Pacific contracts.

8.2 Operations Security. OPSEC is a five step analytical process (identify critical information; analyze the threat; analyze vulnerabilities; assess risk; develop countermeasures) that is used as a means to identify, control, and protect unclassified and unclassified sensitive information associated with U.S. national security related programs and activities. All personnel working under this task will at some time handle, produce or process Critical Information or CPI, and therefore all Contractor personnel must practice OPSEC. All work is to be performed in accordance with DoD OPSEC requirements, and in accordance with the OPSEC attachment to the DD254.

8.3 Place of Performance. The places of performance for this task are the following:

- It is anticipated that approximately 80% of the work will take place at SSC Pacific Lab spaces located at Offutt AFB, Nebraska over the course of the contract (base and options).
- It is anticipated that approximately 20% of the work will take place at the contractor’s facilities over the course of the contract (base and options). Work at contractor’s facilities shall require prior Government consent as the majority of the work is anticipated at Government facilities.

8.4 IPv6 Applicability. Per FAR 11.002(g), the applicability of IPv6 to agency networks, infrastructure, and applications specific to individual acquisitions will be in accordance with the agency's Enterprise Architecture (see OMB Memorandum M-05-22 dated August 2, 2005).

9.0 PERFORMANCE CRITERIA

Performance Based Criteria is outlined in the Performance Requirements Summary (PRS).

(End of Summary of Changes)